МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт Министерства внутренних дел
Российской Федерации»

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«ПЕРВОНАЧАЛЬНЫЙ ЭТАП РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнила
Аглетдинова Диана Ленаровна,
обучающаяся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2017 года набора, 711 учебного взвода

Руководитель
начальник кафедры криминалистики
кандидат юридических наук,
Нугаева Эльвира Дамировна

К защите _____
рекомендуется / не рекомендуется
Начальник кафедры _____ Э.Д. Нугаева
подпись
Дата защиты «___» _____ 2022 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

С переходом к информационному обществу, наше государство получило широкое распространение информационных систем, электронных средств, беспроводных технологий связи, телекоммуникационную сеть Интернет. Если раньше ко всему вышеперечисленному имели доступ лишь единицы, то сейчас это может сделать каждый. Теперь для получения государственных и муниципальных услуг нет необходимости, подолгу стоять в очереди, достаточно взять в руки телефон и получить услуги в электронном виде.

Все большее количество персональной информации помещается в информационные системы: посредством электронных сервисов пересылаются фотографии, копии документов, удостоверяющие личность, для оплаты различных покупок вносятся реквизиты банковских карт, в социальных сетях можно найти информацию о личной жизни каждого человека, посредством мессенджеров передается иная конфиденциальная информация.

Вследствие того, что происходит достаточно быстрое внедрение этих систем, государство не успевает устанавливать защитные правовые механизмы.

По данным статистики Министерства внутренних дел Российской Федерации за отчетный период январь-апрель 2022 года. В январе-апреле 2022 года зарегистрировано 124,2 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 8,5% меньше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес уменьшился с 27,1% до 25,7%. Практически все такие преступления (98,5%) выявляются органами внутренних дел. Больше половины таких преступлений (54,0%) относится к категориям тяжких и особо тяжких (67,1 тыс.; -14,4%), почти три четверти (72,0%) совершается с использованием сети «Интернет» (89,5 тыс.; +4,3%), более трети (39,7%) – средств мобильной связи (49,3 тыс.; -9,1%). Почти три четверти таких преступлений (72,7%)

совершается путем кражи или мошенничества: 90,4 тыс. (-10,3%), каждое десятое (10,9%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 13,6 тыс. (-9,2%)[1] . Данные статистики позволяют сделать вывод о том, остается большой процент не раскрытых преступлений. Расследование данных видов преступлений зачастую не приносит успешного результата (лицо, совершившее преступление не устанавливается, не привлекается к уголовной ответственности, возникает сложность в установке местонахождения, лица совершившего преступление и т.д). Вследствие этого, современные способы совершения преступлений требуют современных методов раскрытия и расследования.

Таким образом, возникает необходимость рассмотрение теоретических и практических вопросов методики расследования мошенничеств, совершенных с использованием информационно-телекоммуникационной сети Интернет, компьютерной информации, и разработка научно-обоснованных рекомендаций и рациональных способов организации раскрытия и расследования данного вида преступлений, отвечающих современному уровню развития информационных технологий, достижений криминалистической науки, общей теории судебных экспертиз.

Цель исследования предопределила необходимость постановки следующих исследовательских задач:

1) проанализировать криминалистическую характеристику мошенничеств, совершенных с использованием телекоммуникационной сети Интернет на основании научных и эмпирических данных;

2) выявить на основании статистических данных основные способы совершения преступления и обстоятельства, способствующие совершению преступления;

3) определить основные механизмы образования следов при совершении

---

[1] Состояние преступности в России // МВД РФ ФКУ «Главный информационно-аналитический центр». М., 2022. С. 30.

данного вида преступлений;

4) проанализировать порядок взаимодействия подразделений следственных органов с различными службами при расследовании уголовных дел изучаемой категории;

5) изучить состояние следственной и судебной практики по уголовным делам о преступлениях с использованием телекоммуникационной сети Интернет;

6) определить задачи первоначального этапа расследования;

7) выявить типичные следственные ситуации мошенничества в сети Интернет.

8) проанализировать тактику производства отдельных следственных действий в зависимости от типичных исходных следственных ситуаций, последовательно складывающихся на первоначальном этапе расследования;

Объектом работы является преступная деятельность лиц, совершающих мошенничеств, совершенных с использованием телекоммуникационной сети Интернет и деятельность лиц, уполномоченных вести раскрытие и расследование данного вида преступлений.

Предметом данной работы являются механизмы совершения данного вида преступлений, основные источники получения информации о преступлении, а также закономерности собирания, исследования, оценки и использования доказательств в расследовании обозначенных преступлений.

Методами изучения данной темы являются совокупность различных методологических приемов, средств познания и эмпирического исследования. Так, применялись и использовались общие и частно-научные методы познания:

1. Системно-структурный анализ: (изучение отдельных норм и положений нормативно-правовых актов, регламентирующих особенности деятельности в информационно-телекоммуникационной сфере и ответственности за их нарушение, а также особенностей деятельности должностных лиц, осуществляющих расследование нарушений в указанной

сфере);

2. Ситуационный: обобщение и описание (обобщение полученных статистических и иных данных, описание их влияния на процесс расследования рассматриваемой категории преступлений);

3. Сравнение: (влияние особенностей деятельности лиц, совершающих мошенничество в информационно-телекоммуникационной сети Интернет и лиц, осуществляющих их расследование) и иные методы.

Выпускная квалификационная работа включает себя введение, три главы, девять параграфов, заключение и список использованной литературы.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ

§ 1. Общая характеристика преступлений: криминалистический и уголовно-правовой аспекты

Данная разновидность преступлений, как и большинство преступлений в информационно-коммуникационной сети Интернет, обладает высокой латентностью. Во-первых, имеются проблемы в расследовании данного вида преступлений, а также возникает сложность в установлении субъектов преступления, механизмов следообразования и других немаловажных криминалистических характеристик преступления. Во-вторых, имеется достаточное большое количество мошеннических схем в Интернете, которые постоянно обновляются. В-третьих, отсутствие качественных специалистов, разбирающихся в данной категории преступлений, поскольку, это больше техническая сфера.

В Уголовный кодекс Российской Федерации термин «мошенничество» был введен федеральным законом в 2003 году. Мошенничество характеризуется как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, а также совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину; совершенное лицом с использованием своего служебного положения; совершенное организованной группой либо в особо крупном размере)[1].

Условиями и причинами внесения изменения в Уголовный кодекс Российской Федерации стали увеличение числа новых категорий преступлений,

---

[1] Никульченкова Е. В. Мошенничество проблемные вопросы // Вестник Омского университета. Серия «Право». 2016. № 2. С. 160.

а именно появление ранее неизвестных мошеннических схем.

Законодательную инициативу в данном вопросе проявил Верховный Суд РФ. Вносимые в Государственную Думу РФ законодательные новеллы были им обоснованы следующим образом: «...по нашему мнению, конкретизация в Уголовном кодексе Российской Федерации составов мошенничества в зависимости от сферы правоотношений, в которой они совершаются, снизит число ошибок и злоупотреблений во время возбуждения уголовных дел о мошенничестве, будет способствовать – повышению качества работы по выявлению и расследованию таких преступлений, – правильной квалификации содеянного органами предварительного расследования и судом, – более четкому отграничению уголовно наказуемых деяний от гражданско-правовых отношений»[1].

В 2013 году Федеральным законом 08.12.2003 №162-ФЗ были внесены изменения в Уголовный кодекс Российской Федерации. Особенная часть УК РФ была дополнена статьями 159.1 «Мошенничество в сфере кредитования», ст. 159.2 «Мошенничество при получении выплат», ст. 159.3 «Мошенничество с использованием платежных карт», ст. 159.5 «Мошенничество сфере кредитования», ст. 159.6 «Мошенничество в сфере компьютерной информации.

Необходимость введения изменения обуславливалась несколькими причинами. В первую очередь, это увеличение числа преступлений с использованием информационно-телекоммуникационных сетей. Поскольку старая версия УК РФ не предполагала наличие таких составов преступления и соответственно отсутствовала мера наказания.

Однако проблема в применении вышеуказанных статей все еще существовала. Так, при квалификации и разграничении кражи и мошенничества с использованием сети Интернет судебная практика складывалась самым разнообразными способами.

---

[1] Досье на проект Федерального закона № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации (в части дифференциации мошенничества на отдельные составы)» // Гарант: информ.-правовой портал. URL: www.garant.ru (дата обращения: 04.04.2022).

Для подтверждения выдвинутого тезиса, приведем конкретные примеры из судебной практики. Приговором Туймазинского межрайонного суда Республики Башкортостан С.А.Р. признали виновным в совершении преступлений, предусмотренных ч.1 ст. 159.6 УК РФ и ч.1 ст. 161 УК РФ. С.А.Р. воспользовался похищенным сотовым телефоном, в целях незаконного завладения чужими денежными средствами, в котором было установлено приложение «Сбербанк», посредством которого был осуществлен перевод денежных средств на его собственный телефон. В результате со счета банковской карты «Сбербанк» у потерпевшего были списаны денежные средства. Суд, вменяя состав преступления, предусмотренный ст.159.6 УК РФ, учитывал, что перевод денежных средств на соответствующий номер, представлял собой ввод компьютерной информации в форме сигнала, что являлось способом совершения мошеннических действий и, следовательно, образовывало соответственно состав мошенничества использованием информационно-телекоммуникационной сети Интернет[1].

Аналогичная ситуация была квалифицирована судом совсем иначе. В приговоре от 10.04.2018 года Калининским районным судом г.Челябинска. П.М.Ю. посредством перевода денежных средств с банковского счета потерпевшего на подконтрольный ему абонентский номер, в целях хищения чужих денежных средств, завладел похищенными денежными средствами.

Суд, рассмотрев материалы дела, назначил обвиняемому наказание за совершение деяние по п. «в» ч.2 ст. 158 УК РФ, то есть хищение денежных средств с причинением значительного ущерба гражданину[2]. Как видно из вышеизложенных приговоров, у суда отсутствует единообразный подход при квалификации идентичных деяний[3].

---

[1] Приговор Туймазинского межрайонного суда Республики Башкортостан от 18.04.2019 № 1-30/2019 // URL: https://sudact.ru (дата обращения: 04.04.2022).

[2] Потапова А. В. Мошенничество в сети интернет: криминологическая характеристика и проблемы квалификации. Научно-образовательный журнал для студентов и преподавателей. // Право. 2020. № 5. С. 45.

[3] Решение Калининского районного Суда г. Челябинска (Челябинская область) от 18.04.2018 г. № 2а-1975/2018. // URL: https://sudact.ru (дата обрашения: 04.04.2022).

Исходя из разъяснений, представленных в постановлении Пленума Верховного Суда РФ, возникает вопрос о возможности применения статьи 159.6 УК РФ, так как часто встречающиеся случаи из практики, которые ранее квалифицировали по ст.159.6 УК РФ, теперь необходимо квалифицировать по статьям 158 УК РФ.

Каждое преступление имеет свои особенности и присуще ему черты, совокупность взаимосвязанных между собой элементов определяется как криминалистическая характеристика преступления.

Определенному виду преступления присуще индивидуальная совокупность элементов криминалистической характеристики, которые закономерно взаимосвязаны между собой. Достаточные объективные данные о некоторых особенностях и признаках преступления позволяют эффективно решать задачи первоначального и последующего этапа раскрытия и расследования преступлений. Значимость криминалистической характеристики преступлений в своей работе указывал А.А. Бессонов, в ходе опроса практических работников 99% опрошенных признали ее практическую ценность для получения информации о типичных способах совершения преступления (39 %), следах преступления и наиболее вероятных местах их обнаружения (27 %)[1].

В ходе изучения научной литературы, были определены наиболее значимые элементы криминалистической характеристики мошенничеств, совершаемых с использованием информационно-телекоммуникационной сети Интернет:

1) механизм и обстоятельства совершения преступления;

2) криминалистически значимые особенности личности преступника и потерпевшего;

3) криминалистически значимые данные о механизме следообразования.

Основными направлениями использования криминалистической

---

[1] Бессонов А. А. О сущности криминалистической характеристики // Вестник Поволжской академии государственной службы. 2014. № 6 (45). С. 48.

характеристики данного вида мошенничества являются:

1. Установление и поиск доказательств путем изучения взаимосвязи сведений о механизме, обстановке и личности подозреваемых и потерпевших. В дальнейшем, эта информация может помочь в установлении еще неизвестных следственным органам потерпевших;

2. Выдвижение следственных версий на основе одной из криминалистических характеристик. На основе информации о том, что мошенничества, совершенных с использованием информационно-телекоммуникационной сети Интернет совершаются зачастую лицами мужского пола, ранее не судимыми, в возрасте 18-30 лет, можно заметно, сузить круг лиц, подозреваемых в совершении преступления;

3. Определение тактики проведения следственных действий и оперативно-розыскных мероприятий. Так, получив информацию о личности подозреваемого можно составить план проведения допроса, узнать о возможном сопротивлении со стороны подозреваемого.

4. Профилактика и предупреждение преступлений. Анализируя личности потерпевших можно сделать вывод о том, кто чаще всего становиться жертвой данных преступлений, в дальнейшем провести работу по предупреждению преступлений среди выявленных лиц.

§ 2. Криминалистически значимые особенности личности потерпевшего и личности преступника

Анализ личности поведения потерпевшего, личности преступника позволяет получить информацию о механизме, способах совершения преступления, а также разграничить мошенничество в сети Интернет от других видов мошенничеств. Для начала нужно разобраться, что подразумевается под словом «потерпевший». Потерпевший – это физическое лицо, которому в результате причинен физический, имущественный или моральный вред, а также юридическое лицо, которому в свою очередь причинен вред имуществу и

деловой репутации[1].

Анализ личности жертвы преступления позволит следователю определить тактику проведения отдельных следственных действий, разработать следственные действия.

Б.А. Куринов верно отмечает, что «первоочередное значение для раскрытия личности потерпевших от мошенничества имеют социально-демографические признаки (пол, возраст, образование, социальное и семейное положение)»[2].

Изучая сведения о потерпевшем, необходимо учитывать половозрастные характеристики, семейное положение, образование, род занятий, его отношения с преступником на момент совершения преступления, а также состояние потерпевшего в момент совершения преступного деяния.

В ходе анализа следственной и судебной практики было установлено, что наибольшее число преступлений по данным видам преступлений совершается в отношении лиц, по следующим возрастным характеристикам:

1) от 40 до 50 лет – 41%;
2) от 30 до 40 лет – 39%;
3) старше 50 лет – 8%;
4) до 30 и до 18 лет – равное количество – по 5%.

Подобная возрастная градация обусловлена несколькими причинами. Во-первых, мошенничество с использованием информационно-телекоммуникационной сети Интернет имеет свою специфику. Необходимо использовать смартфон с доступом к Интернету, пользоваться мобильными приложениями и банковскими картами. Например, по некоторым видам мошенничеств, совершенных с использованием информационно-телекоммуникационной сети Интернет необходимо переводить денежные

---

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – 20 июня.

[2] Тарубаров В. В. Общественные места как участки местности с повышенной социальной опасностью // Вестник Московского университета МВД России. 2015. № 1. С. 115.

средства с использованием мобильного банка. Лица, старше 50 лет не в достаточной мере освоили данную сферу, имеют сложности в обращении с технической аппаратурой. Лица, до 18 лет и 30 лет более осведомлены в данном вопросе, коммуникативные, достаточные активные пользователи социальных сетей и имеют информацию о возможности совершении мошенничеств.

Не менее важными представляются сведения о взаимоотношениях преступника и потерпевшего до момента совершения преступного деяния и в самой ситуации совершения преступления. В большинстве случаев, в 80%, жертва и преступник были незнакомы.

Потерпевших от мошенничества можно разделить на две основные группы, исходя из активности их поведения и после получения информации о том, что они стали жертвами мошенников[1]:

1. Потерпевшие, заинтересованные в успешном расследовании преступления, предоставляющие правоохранительным органам всю известную им информацию и осуществляющие активное содействие в иных формах;

2. Потерпевшие с пассивным поведением. Представители данной группы чаще всего не заинтересованы в исходе уголовного дела, их цель – написать заявление в правоохранительные органы, и на этом как они считают, их роль окончена.

Целесообразно выделить еще одну группу потерпевших, лица, которые скрывают свой статус потерпевшего, даже в некоторых случаях склонны к оказанию сопротивления правоохранительным органам. Данное поведение обуславливается рядом причин: страх за раскрытие личных данных, в отсутствии веры в успешное раскрытие и расследовании преступлений. Указанная группа потерпевших чаще всего не верят в нахождении и установлении лица совершившего преступление. Вследствие этого, возникает такое явление как латентность преступлений.

По данным статистики МВД России количество заявлений о

---

[1] Никулин Д. В. Жертвы мошенничества // Научно-практический электронный журнал Аллея науки. 2018. № 1. Ст. 10.

мошенничестве в 2022 году выросло, на 5,1 % по сравнению с 2021 годом превысив 249 тысяч. Результаты статистики позволяют сделать вывод о том, что количество лиц, заявляющих, по данным видам преступлений становится больше. В этом случае, можно выделить два фактора, способствующие росту данного явления:

1. Рост указанного вида преступлений;

2. Увеличение числа потерпевших, заинтересованных в привлечении лиц, совершающих преступления.

Однако существенная проблема в данной области существуют. Возникает необходимость проведения работы по повышению доверия к правоохранительным органам. Решение данной проблемы позволит привлекать большее количество потерпевших к сотрудничеству в расследовании, а также обладать более полной информацией и, следовательно, более качественно расследовать мошенничества с использованием информационно-телекоммуникационной сети Интернет.

В ОМВД России по Туймазинскому району обратился гражданин А.Т.И. с заявлением о том, что к нему по телефону обратились неизвестные люди, которые представились сотрудниками банка. Они сообщили, что на гражданина А.Т. И. пытаются оформить кредит. Поэтому, ему необходимо оформить другой кредит, снять деньги и положить на счет «QIWI» кошелька. В результате, данное лицо положило на вышеуказанный счет около миллиона рублей. На вопрос следователя в ходе допроса: «Знали ли вы, о том, что в настоящий момент данная мошенническая схема распространена? Имеются достаточное количество потерпевших, информация транслируется по новостям». Ответ потерпевшего: «Нет, телевизор не смотрю. Никто об этом мне не рассказывал».

Проведение такой работы особенно актуально для предупреждения и профилактики преступлений. В особенности агитационная работа проводится сотрудниками Министерства внутренних дел РФ, демонстрация видеороликов, раздача листовок «Осторожно-мошенники!», профилактическая беседа с

гражданами. В таких случаях, работа по информированию населения позволит обратить внимание на текущую криминальную обстановку и быть в курсе о наиболее серьёзных угрозах на данный момент, и позволит не стать жертвой преступника.

Одним из немаловажных элементов криминалистической характеристики преступлений является информация о личности преступника. Обобщая криминалистическую литературу, можно сказать, что изучение личности преступника предполагает раскрытие структуры этой личности, представляющей собой упорядоченное соотношение свойств (признаков), характеризующих нарушителя правового запрета.

Данная структура включает в себя шесть групп признаков[1]:

1) социально-демографические признаки (пол, этническая принадлежность, возраст и др.);

2) социальные признаки, проявляющиеся в различных сферах жизнедеятельности (например, профессия или семейное положение);

3) нравственные признаки (отношение к религии и др.);

4) уголовно-правовые признаки (наличие судимости и др.);

5) физические признаки (наличие заболеваний и др.);

6) психологические признаки.

Особое значение в свете рассмотрения данного вопроса рассматривал В.Б. Вехов, он выделял три группы преступников[2]:

1) лица, которые отличаются профессионализмом в сфере интернет технологий;

2) лица, имеющие психические отклонения, вызванные компьютерными фобиями и информационным болезнями;

3) профессиональные мошенники в сети Интернет с явными корыстными интересами.

---

[1] Русаков И. М. Криминалистическая характеристика личности преступника, совершившего мошенничество в сфере предоставления интернет-услуг // Вестник Краснодарского университета МВД России. 2018. № 4. С. 206.

[2] Козлов В. Е. Теория и практика борьбы с преступностью. М., 2017. С. 54.

Взаимодействие свойств (особенностей) личности лица, совершившего преступление, и обстановки, в которой было совершено преступление, находит свое внешнее проявление в конкретном преступном поведении.

Анализ следственной практики показывает, что чаще всего лицами, совершающими, преступления с использованием информационно-телекоммуникационной сети Интернет является, преобладание лиц мужского пола. Причины заключаются в том, что мужчины обладают более высокой социальной активностью, быстрее приспосабливаются к изменением, происходящим в обществе.

Анализ криминалистической литературы и следственной практики позволяет сделать вывод о том, что большинство мошенничеств совершаются моложе 34 лет. Средний возраст лиц, совершающих варьируется от 18 до 30 лет. В качестве примера, подтверждающего приведенные цифры, можно указать результаты, полученные в результате изучения уголовных дел. Изучив личности 11 преступников, были получены такие выводы по следующим возрастным категориям:

1) до 18 лет - 2 человека (18%);

2) 18-30 лет - 8 человек (72%);

3) 30-45 лет - 1 человек (9%);

4) 45 лет и старше - 0 человек (0%)[1].

Таким образом, именно лица мужского пола среднего возраста зачастую совершают мошенничества с использованием информационно-телекоммуникационной сети Интернет. Другой важной характеристикой является наличие образования, большинство преступников имеют высшее и среднее образование. В процессе расследования преступлений следователь запрашивает характеристику о наличии или отсутствии судимостей подозреваемого лица. Анализ данных характеристик показывает, что практически все подозреваемые не имеют судимостей. Данная особенность

---

[1] Романова Л. И. Личность интернет-преступника //Азиатско-Тихоокеанский регион: экономика, политика и право. 2018. № 3. С.159-169.

отличает мошенничество в сети Интернет от других видов преступлений. Поскольку в остальных случаях, лицо совершает преступление повторно. Это объясняется тем, что этот вид мошенничества является относительным новым видом преступления.

Однако в криминалистической литературе отмечается, что лица, ранее совершившие преступления, отбыв наказание, могут вновь поступить к преступным действиям. Так как, со временем будут появляться новые, более эффективные возможности для совершения преступных посягательств. Определяющей особенностью личности мошенника в сети Интернет является их информационно-технические навыки работы в удаленном от места преступления, корыстные интересы, способность вызывать доверие у людей.

Таким образом, личность подозреваемого в совершении мошенничеств с использованием информационно-телекоммуникационной сети Интернет имеет свои специфические особенности, присущие ему только черты. Возникает необходимость выделить криминалистическую характеристику личности преступника в отдельную специфическую категорию. Сущность этих высказываний сводится к тому, что они имеют информационно-технические навыки работы в удаленном от места происшествия доступе, корыстные интересы, склонность к творческим изобретениям при разработке преступных схем, способность вызывать доверии у людей.

§ 3. Способы и обстановка совершения преступления

Для каждого преступления присущ свой набор действий и механизмов. Анализ на месте преступления обстоятельств, произошедшего, изучение преступных действий подозреваемого позволяет разработать следственные версии, определить тактику проведения следственных действий и оперативно-розыскных мероприятий.

Один из главных элементов мошенничества, совершенного с использованием Интернет, несомненно, является способ совершения

преступления.

Способ совершения преступления, по мнению М.И. Еникеева, представляет собой систему приёмов, действий, операционных комплексов, обусловленных целью и мотивами действия, психическими и физическими особенностями действующего лица, в котором проявляются психофизиологические и характерологические особенности человека, его знания, умения, навыки, привычки и отношение к различным сторонам действительности. Для каждого преступления существует свой системный «набор», комплекс действий и операций. У каждого человека также имеется система обобщённых способов действий, свидетельствующих об его индивидуальных особенностях[1].

Способ совершения преступления:

1) определяется этапам подготовки, большая часть мошенничеств, совершаются с предварительной подготовкой, которая заключается в поиске жертвы; создание непосредственных условий совершения. С этой целью, преступник входит в доверие к потерпевшему, и путем обмана пытается сформулировать желание на совершение определенных действий;

2) непосредственным совершением преступления;

3) этап сокрытия преступления.

В результате анализа информации, полученной из различных источников, а также изучение следственной практики позволило выделить наиболее распространенные виды и способы мошенничеств:

1) преступления с использованием услуги «Мобильный банк» посредством мобильной связи:

Телефон выбывает из владения собственника по различным причинам (утрата телефонного аппарата либо его хищение), при этом потерпевший не отключает услугу «Мобильный банк» от сим-карты и преступник получает

---

[1] Большакова В. Н. Разграничение криминалистических понятий: модель преступления, поисковый портрет преступника, криминалистическая характеристика преступлений // Пробелы в российском законодательстве. 2014. № 3. С. 52.

возможность производить манипуляции с денежными средствами, пользуясь данной услугой;

В ходе изучения уголовных дел было установлено, что А.Г.В. потерял телефон, нашедший вытащил из него SIM-карту, зашёл в мобильный банк «Сбербанка» с помощью номера просроченной карты и вывел со счёта 115 тысяч рублей. Спустя время, он обнаружил, что неизвестный перевёл 115 тысяч рублей на карту незнакомого ему человека. Деньги были переведены в пять операций: сначала восемь тысяч, затем 48 тысяч, 37 тысяч, 20 тысяч и две тысячи рублей. С помощью выписки по SIM-карте и службы безопасности «Сбербанка» А.Г.В. узнал, что неизвестный отправил более 70 SMS на номер банка 900, после чего вошёл в мобильный банк по номеру старой карты. В ходе допроса А.Г.В. пояснил, что предполагает, что злоумышленник получил номер карты по обращению на номер 900, запросил одноразовый пароль для доступа к финансам[1];

2) потерпевшим производится замена номера телефона, при этом сим-карта остается прежней, либо потерпевшим в течение нескольких месяцев сим-карта с подключенной услугой «Мобильный банк» не используется, после чего продается компанией сотовой связи новому владельцу, который, получая смс-сообщения с номера «900», имеет возможность осуществлять операции с денежными средствами на счетах.

Ярким примером может послужить приговор Орджоникидзевского районного суда г. Новокузнецка Кемеровской области. Б.В.Н., получив сообщение с номера 900 о пополнении баланса банковского счета незнакомой ему гражданской, достоверно зная, что пополнения счета его банковской карты не было, с банковского счета Ф.А.Р., реализуя свой внезапно возникший преступный умысел, используя мобильный телефон, посредством услуги «Мобильный банк», с банковского счета банковской карты Ф.А.Р. перевел денежные средства 100 рублей на счет своего мобильного телефона. Затем,

---

[1] Уголовное дело № 119…111 // Арх. СО ОМВД России по Туймазинскому району. С. 3-19

действуя в продолжение своего преступного умысла, используя мобильный телефон, посредством услуги «Мобильный банк», с банковского счета банковской карты Ф.А.Р. перевел денежные средства 2050 рублей на банковский счет банковской карты, принадлежащий А.М.А., тем самым похитил денежные средства, принадлежащие Ф.А.Р. в размере 2150,0 рублей. В свою очередь были даны показания потерпевшей Ф.А.Р. из которых следует, что около 1,5 года назад ее дочь на свое имя оформила банковскую карту, к которой привязала свой номер телефона, и подключила к данному номеру телефона услугу «Мобильный банк». Она положила на банковскую карту дочери 1700 рублей, у нее на счету еще имелись денежные средства около 450 рублей и когда она дочери положила 1700 рублей через услугу «Мобильный банк», у нее стало 2150 рублей. Позже от дочери узнала о том, что в баланс на карте оказался равен нулю, хотя на карте должна была находиться 2150 рублей. Дочь пришла домой и увидела, что все деньги на карте были сняты, а именно: 100 рублей переведены на номер телефона, а остальные деньги переведены на номер карты. Таким образом, с карты ее дочери были сняты деньги в размере 2150 рублей, которые принадлежат ей[1];

3) путем внедрения вирусов;

Путем обмана через смс-сообщения о блокировке карты, имеющейся задолженности, либо об отсутствии денежных средств на карте, либо о заявке на перевод денежных средств с указанием контактного телефона. Мошенник сообщает, что «банк выявил подозрительную операцию» или «в системе произошел сбой». Он просит у вас полные данные карты, CVV- или CVC-код, код из СМС или пароли мобильных банков. Это нужно якобы «для сохранности денег».

4) путем обмана через звонок потерпевшему лицу.

Лицо, представляется сотрудником банка и сообщает о том, что на него

---

[1] Приговор Орджоникидзевского районного суда г. Новокузнецка Кемеровской области № 1-26/2019 1-362/2018 от 15 февраля 2019 г. по делу № 1-26/2019 // Судебные и нормативные акты РФ. // URL: https://sudact.ru (дата обращения: 04.04.2022).

«мошенники» хотят оформить онлайн кредит. Чтобы предотвратить это, жертву убеждают самому оформить кредит на ту же сумму, после чего обналичить поступившие средства и перечислить их на так называемый резервный счет для мгновенного погашения долга.

В ходе изучения уголовных дел, данный способ был подтвержден уголовным делом расследуемый СО ОМВД России по Туймазинскому району. В дежурную часть обратился Г.Д.Н. с заявлением о том, что ему на телефон позвонили и представились сотрудниками «Сбербанка». Ему сообщили, что на него пытаются оформить кредит около 700 тыс. рублей. Для того чтобы сразу погасить данный кредит ему необходимо оформить новый. Затем, снять указанные средства и положить на «QIWI» кошелек, счет которого они сообщат. Г.Д.Н. все указанные действия совершил. Следствием было установлено, что деньги были переведены на счет мошенников, тем самым он лишился 700 тыс. рублей[1];

5) наиболее распространенным способом мошенничества является как заведомо фиктивная продажа или покупка товаров, а также предоставление услуг. Преступник размещает объявление о продаже товаров или предоставление услуг на интернет-сайтах и в социальных сетях. Чаще всего это сайты «Авито» «Юла», либо непосредственно в самой социальной сети. После того как лицо откликается на объявление, ему предлагается перечислить денежные средства за товар или услугу в качестве предоплаты либо полной оплаты. После того как потерпевший перечислит указанную сумму, преступник либо удаляет «профиль», либо просто перестает выходить на связь.

По данному сценарию мошенничества Советским районным судом г. Уфы Республики Башкортостан был осужден г-н Ю.В.Т., умышленно, из корыстных побуждений, с целью хищения чужого имущества, выложил объявление на сайте «Авито», о продаже металлического профилированного листа. Изначально не намереваясь выполнить свои обязательства, так как

---

[1] Уголовное дело № 119…118 // Арх. СО ОМВД России по Туймазинскому району. С. 5-18.

заведомо знал, что у него не имеется в наличии металлического профилированного листа и отсутствует реальная возможность осуществить его поставку, но в ходе телефонного разговора, используя обман, убедил С.М.Р. приобрести у него данный материал на условиях 100% предоплаты. Ю.В.Т. обязался поставить для С.М.Р. оцинкованный профнастил на общую сумму 18 000,00 руб.

Будучи обманутым, не подозревая о преступных намерениях Ю.В.Т., исполняя условия договора полностью, С.М.Р., используя услугу «Сбербанк Онлайн» перевела деньги в сумме 18 000,00 руб., на карту ПАО Сбербанк России, номер которой Ю.В.Т. прислал СМС-сообщением. Ю.В.Т. Полученные от С.М.Р. денежные средства он в дальнейшем похитил и использовал по своему усмотрению в личных интересах. При этом, как и предусматривалось преступным умыслом Ю.В.Т., вышеуказанный строительный материал С.М.Р., предоставлен не был[1].

Исходя из специфики мошенничеств, совершенных с использованием информационно-телекоммуникационной сети «Интернет» особый интерес вызывают такие элементы криминалистической характеристики, как место и время совершения преступления.

Возникает необходимость их более подробного рассмотрения. Традиционно под определением места совершения преступления признается то место, где произошло деяние, значимое в криминалистическом и уголовно-правовом отношении.

В рассматриваемых преступлениях большое значение имеет местоположение преступника. Вследствие того, что используемые технологии удаленного доступа, электронных расчетов, вредоносных программ не

---

[1] Приговор Советского районного суда г. Уфы Республики Башкортостан № 1-26/2019 1-362/2018 от 07 мая 2019 г. по делу № 1-26/2019 // Судебные и нормативные акты РФ. // URL: https://sudact.ru (дата обращения: 04.04.2022).

совпадают с реальным местоположением, как самого преступника, так и с местом совершения преступления[1].

Место совершения преступления характеризуется двумя составляющими: местоположение в реальном пространстве (местонахождение физического лица, организации) и местоположением, которое постоянно отождествляется в локальной и глобальной сети с уникальным номером IP-адресом.

Анализируя вышесказанное, под местом совершением преступления определяется место нахождения преступника в момент или период осуществления акта преступного действия, так и место нахождения аппаратных и программных средств, используемых в процессе расследования преступлений. Эту характеристику необходимо учитывать при проведении и процессуальном оформлении осмотра места происшествия.

Изучение уголовных дел мошенничеств в сети Интернет показало, что преступления могут совершаться в любое время суток вне зависимости от времени года, что не характерно для других видов преступлений.

Необходимо отметить, что выявление основных способов мошенничеств с использованием информационно-телекоммуникационной сети Интернет дает информацию о других криминалистических характеристиках преступления и помогает следственным органам выдвигать следственные версии.

§ 3. Механизм следообразования

Мошенничество, совершенное с использованием информационно-телекоммуникационной сети Интернет, оставляет определенные характерные следы. Установление механизма следообразования способствует выяснению обстоятельств, случившегося, выдвижению следственных версий, а также обнаружению новых следов преступлений.

---

[1] Олиндер Н. В. Время и место совершения преступлении как элемент криминалистической характеристики преступлений, совершенных с использованием электронных платежных средств и систем // Науковедческие проблемы криминалистики. 2018. № 4. С. 17.

В ходе изучения научной литературы были выявлена следующая классификация следов преступлений:

1. По способу возникновения:

а) идеальные следы (показания участников уголовного судопроизводства);

Например, в ходе изучения следственной и судебной практики мошенничества с использованием интернет-магазина, который впоследствии был заблокирован и недоступен для просмотра. Благодаря показаниям потерпевших органам предварительного следствия удалось получить информацию о наименовании, адресе, контактных данных, указанных на данном сайте, что способствовало установлению подозреваемых.

б) материальные следы (любые материальные последствия, возникшие после совершения преступления).

3. По времени возникновения:

а) следы, образованные на подготовительном этапе мошенничества (подбор технического оборудования, поиск жертвы преступления);

б) следы, образованные на рабочем этапе совершения преступления (выписки банковских операций, звонки потерпевшим лицам);

в) следы, оставленные на заключительном этапе преступления (отпечатки пальцев рук, следы уничтожения документов и т. п.);

Доказательственная информация по мошенничествам с использованием информационно-телекоммуникационной сети Интернет содержится в так называемых «виртуальных следах».

Как показывает практика расследования уголовных дел рассматриваемой категории данная проблема наиболее часто встречающаяся. Важное место занимают именно вопросы выявления пользователей информационно-телекоммуникационного оборудования, в том числе предопределенные активным распространением средств, сокрытия идентификационной информации пользователей сети Интернет, доминированием иностранных аппаратных и программных средств, элементной базы, IP-адресов, серверов и

ресурсов, находящихся вне юрисдикции Российской Федерации, что практически полностью исключает возможность получения криминалистически значимой информации.

Рассмотрим на примере следственной практики, Х.Д.Ф. обратился с заявлением в дежурную часть отдела полиции города Н. о том, что в отношении него было совершены мошеннические действия. Х.Д.Ф. на сайте «Авито» намеревался приобрести товар, для подтверждения своих действий продавец предложил внести Х.Д.Ф. предоплату. После внесения предоплаты продавец исчез, а товар не был передан. В ходе проведения оперативно-розыскных мероприятий было установлено, что деньги были переведены на счет, чей владелец на момент получения денежных средств находился в Соединенных Штатах Америки.

Кроме того, типичными следами по данным видам мошенничества могут быть следующие:

1. Оргтехника:

а) электронная (компьютеры, ноутбуки, модемная аппаратура, WI-FI роутеры, техника, направленная на перехват информации);

б) коммуникационная (мобильная, стационарная, электронная почта);

2.Сим-карты, используемые преступниками и Сим-карты потерпевших.

3. Банковские карты, используемые мошенниками при обналичивании денежных средств.

4. Видео- и аудиоматериалы:

а) с камер наблюдения в местах обналичивания мошенниками денежных средств;

б) чаты на сайтах по продажам товаров, голосовые сообщения (см. рис.1).

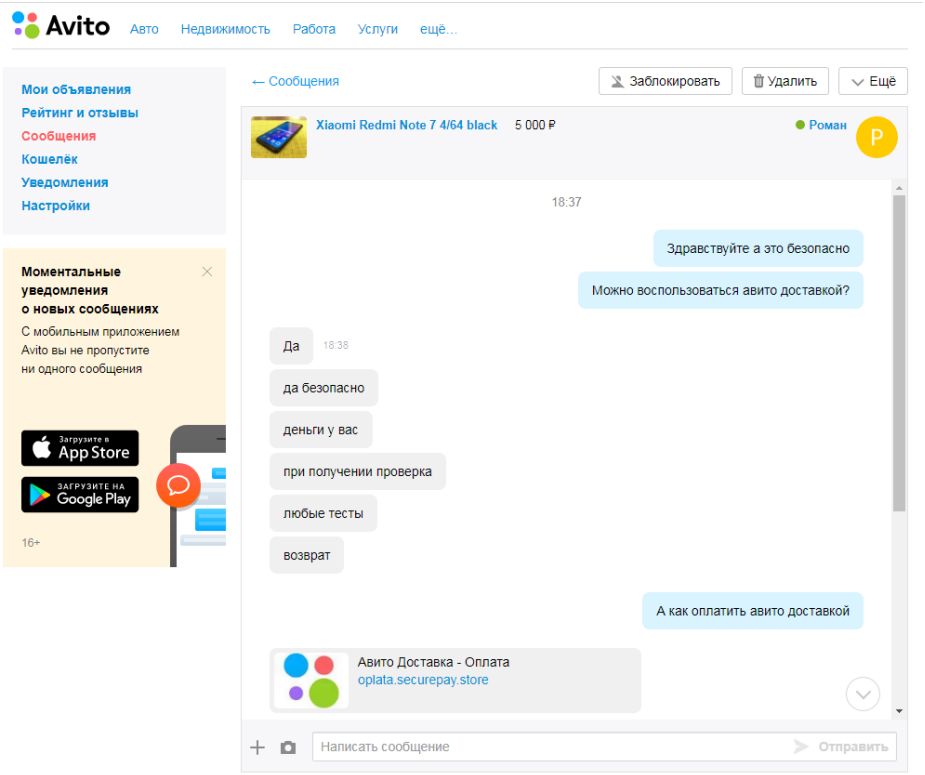

Рис.1. Чат покупателя с продавцом товара

6. Сведения, запрашиваемые сотрудниками органов предварительного расследования у соответствующих служб, организаций:

а) о местонахождении мобильных устройств в момент совершения преступления, предоставленные операторами мобильной связи;

б) обо всех онлайн-кошельках и интернет-страницах, онлайн-кабинетах, привязанных к номерам преступников, с подтверждением поступления на данные счета денежных средств и выполненных операций;

в) об IP-адресах, о соединениях, операциях по ним за весь имеющийся период с указанием фактических адресов, с которых происходила авторизация участника в сети Интернет, а также поступление денежных средств на счета;

г) детализация телефонных соединений, адреса базовых станций по указанным SIM-картам и телефонам.

Обобщая изложенное, отметим, что применительно к расследованию мошенничеств, совершенных с использованием информационно-телекоммуникационной сети Интернет количество материальных и идеальных следов индивидуально и находится в непосредственной зависимости от способа совершения преступления и участников преступного деяния. Установление

механизм следообразования представление о способах подготовки, совершения и сокрытия преступления, о лицах, причастных к ним, и потерпевших. Как показывает практика, необходимые сведения по уголовному делу можно установить при изучении деяний совершенных аналогичным способом, так как обязательно появляются дополнительные данные, источники, следы, при помощи которых можно установить виновных лиц.

Таким образом, эффективность выявления, раскрытия и расследования мошенничества в сети Интернет во многом зависит от возможностей правоохранительных органов по грамотному обнаружению, изъятию, исследованию следов.

ГЛАВА 2. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ

§ 1. Особенности проведения доследственной проверки

Доследственная проверка – это основанная на законе и подзаконных актах деятельность уполномоченных уголовно-процессуальным законодательством компетентных государственных органов и должностных лиц, направленная на установление достоверности содержащейся в заявлении (сообщении) информации и сбор дополнительных сведений, характеризующих это событие, которые необходимы для принятия законного и обоснованного процессуального решения по поступившему заявлению или сообщению о преступлении[1].

Во исполнение статьи 144 УПК РФ следователь обязаны принять, проверить сообщение о преступлении и принять решение в соответствии с должностным регламентом. Сообщение проверяется в 3-суточный срок. С момента регистрации сообщения о совершении мошенничества до привлечения виновного к уголовной ответственности сотрудники полиции устанавливают обстоятельства произошедшего и собирают доказательственную базу. Проведение первоначальных следственных действий на этапе доследственной проверки позволяет следователю своевременно пресечь новые эпизоды преступлений, задержать преступника.

Доследственная проверка имеет решающее значение поскольку по ее итогу выноситься решение о возбуждении или об отказе возбуждения уголовного дела. Это соответствует ч. 2 ст. 140 УПК РФ, в которой указано, что только наличие достаточных данных о преступлении является основанием для возбуждения уголовного дела, в связи, с чем основными задачами данного этапа являются установление повода и основания для возбуждения уголовного

---

[1] Рарога. А. И. Уголовное право России: две части. М., 2016. С. 17.

дела.

Таким образом, при поступлении информации о совершении мошенничества с использованием информационно-телекоммуникационной сети Интернет следователь принимает меры по предварительной проверке данной информации и последующему вынесению решения.

За 1 полугодие 2021 года в производстве ОВД по Республике Башкортостан находилось 3259 (+1500) преступлений по фактам мошенничеств, совершенных дистанционным способом, в том числе использованием сети Интернет, средств связи и банковских карт, окончено производством 275 преступлений (+133), приостановлено 2823 (+1129) преступлений, процент составил 40,9 % (- 25,9 %).

В целях повышения эффективности оперативно-служебной деятельности по раскрытию и расследованию данного вида преступлений на территории Республики Башкортостан, надлежащего взаимодействия следственных, оперативных и подразделений дознания, а также выявления признаков серийности и многоэпизодности данного вида преступлений приказом от 22.07.2020 №478 МВД по Республике Башкортостан был утвержден Алгоритм взаимодействия территориальных ОВД Республики Башкортостан при раскрытии и расследовании уголовных дел по мошенничествам и хищениям, совершенным с использованием информационно-телекоммуникационных технологий.

Обязанности следователя территориального ОВД РБ, осуществляющего расследование уголовного дела:

1) принимает заявление и опрашивает потерпевшего об обстоятельствах совершенного преступления, при этом устанавливает:

– способ совершения преступления (посредством сотовой связи, платежных карт, сети Интернет);

– место, время, способ хищения денежных средств (списание с банковской карты, переводом посредства банкомата, платежного терминала, посредством услуг «Мобильный банк», услуг Интернет банкинга), номера

абонентских номеров, используемых злоумышленниками, номера расчетных счетов (банковских карт) на которые переведены денежные средства;

– информацию об Интернет-ресурсах, с помощью которого было совершено преступление (сайты, социальные сети) и иную информацию имеющую значения для дальнейшего раскрытия преступления;

– сведение о лице, совершившем преступления, а именно как называл себя во время общения, какие данные о себе сообщил (представился ли сотрудником Банка, кредитного учреждения и т.п), абонентские номера, адреса электронной почты, паспортные данные, особенности речи, голоса;

– размер причиненного материального ущерба, его значительность с учетом имущественного положения, также документальное подтверждение;

Истребует у заявителя:

– детализацию телефонных соединений по входящим и исходящим звонкам по принадлежащему ему абонентскому номеру, в том числе с использованием онлайн-сервисов;

– выписку по движению денежных средств по банковскому расчету, с которого совершено их хищение, в том числе с использованием онлайн-сервисов;

– сотовый телефон, ноутбук, планшет, компьютер, банковскую карту проводит их осмотр с обязательным использованием фотографической съемки, после чего приобщает к протоколу осмотра фототаблицу, а изъятые предметы под сохранную расписку возвращает заявителю;

В зависимости от обстоятельств совершенного преступления, производит осмотр места происшествия, а именно отделения банка, помещения торгового центра, магазина, где установлены банкоматы или платежные терминалы, помещение квартиры, где в момент совершения находился заявился, при наличии видеозаписи, принимает меры, направленные на ее изъятие, а также изымает иные предметы и следы совершенного преступления;

По фактам взлома аккаунтов в социальных сетях устанавливает их владельцев, с целью получения информации об истории посещения страницы

другими пользователями, в том числе их IP-адресов;

При наличии очевидцев совершенного преступления, опрашивает их обстоятельствах совершения преступления;

В случае если при совершении преступления, имел место перевод денежных средств посредством банкомата или платежного терминала и если у заявителя подтверждающие документы, готовит и направляет в банковские и иные учреждения запрос о предоставлении информации о совершенных транзакциях, а также об истребовании видеозаписей;

В течение дежурных суток дает поручение в подразделение уголовного розыска, в том числе по установлению принадлежности абонентских номеров, используемых злоумышленниками, а также банковских карт, на которые были переведены похищенные денежные средства;

В течение дежурных суток, при подтверждении факта совершения преступления, принимает решение о возбуждении уголовного дела по соответствующей статье Уголовного кодекса РФ, в зависимости от обстоятельств совершенного преступления (ст.159, 159.3 УК РФ либо п. «г» ч.3 ст. 158 УК РФ);

Совместно с руководителем следственного подразделения в обязательном порядке вносит данные необходимые сведения в модуль «Мошенничество» СОДЧ ИСОД МВД России;

После возбуждения уголовного дела, в течение суток:

1) готовит и направляет в подразделение уголовного розыска поручение о проведении отдельных следственных действий и оперативно-розыскных мероприятий;

2) выносит постановление о признании потерпевшим лица, которому причинен материальный ущерб, допрашивает в качестве потерпевшего, с постановкой вопросов;

3) направляет на исполнение запросы, не требующие судебных решений, в том числе банки и иные кредитно-финансовые учреждения (организации предоставляющие услуги электронной коммерции) об истребовании выписок

по движению денежных средств, принадлежности счетов, на которые переводились похищенные денежные средства; организации, предоставляющие Интернет-услуги, услуги телефонной связи о принадлежности абонентских номеров, сведений о пользователе аккаунта, ip- адреса, домена, электронной почты, а также вносит ИБД- Ф реквизиты направленных запросов (исходящие номера и даты, с указанием адресатов, куда были направлены запросы);

4) направляет в суд ходатайство в порядке ст. 186.1 УПК РФ об истребовании информации о соединениях между абонентами и абонентскими номерами связи, с целью установления принадлежности абонентских номеров злоумышленников, истребовании детализации по указанным абонентским номерам, а также по абонентскому номеру самого потерпевшего с указанием базовых станций с установлением срока до 180 суток и с предоставлением запрашиваемой информации не реже одного раза в неделю;

5) направляет в суд ходатайство о наложении ареста на имущество, блокировке и аресте денежных средств на лицевых счетах абонентских номеров операторов сотовой связи, банковской карты или иного банковского счета, используемого злоумышленником при совершении преступления;

6) изучает, представленную подразделением уголовного розыска информацию из ИБД-Ф, при наличии признаков серийности, либо совпадений (по абонентским номерам, IMEI-номерам сотовых телефонов, номеров банковских карт злоумышленников) с другими территориальными ОВД Республики Башкортостан, истребует информацию, которая имеет значение для расследуемого уголовного дела, после чего уведомляет в письменном виде руководителя ОВД о возможности соединения уголовных дел в одно производство;

7) направляет начальникам подразделений уголовного розыска, участковых уполномоченных полиции и иных подразделений органов дознания поручения о проведении о необходимых оперативно-розыскных мероприятий, отдельных следственных действий, с указанием конкретных мероприятий и срока исполнения, через регистрацию;

8) при установления факта неумышленного непредставления сведения оператором сотовой компании, составляет рапорт об обнаружении признаков административного правонарушения с последующей регистрацией в КУСП дежурной части ОВД;

9) направляет в отдел «К» БСТМ МВД по РБ поручения о проведении оперативно-розыскных мероприятий, по уголовным делам, возбужденным по преступлениям, относящимся к их компетенции;

10) принимает меры на получение дополнительной информации о результатах исполнения ранее направленных в различные организации и учреждения запросов

11) истребует из судов постановления в порядке ст.186.1 УПК РФ, после чего самостоятельно направляет их для исполнения операторам сотовой связи, либо предоставляет их сотрудникам подразделения уголовного розыска для последующего направления операторам связи, при этом в тексте запроса указывает о необходимости его исполнения в установленном уголовно-процессуальном законодательством РФ срок и разъясняет юридические последствия неисполнения законных требований правоохранительных и судебных органов;

12) после получение ответов на ранее направленные в организации и учреждения, а также операторам сотовой связи запросы, совместно с сотрудниками подразделения уголовного розыска проводит их анализ и в случае получения положительной информации, способствует ее реализации и внесению в ИБД-Ф;

13) при необходимости назначает соответствующие судебные экспертизы, в том числе компьютерные;

14) обеспечивает в процессе расследования каждого уголовного дела выявление обстоятельств, способствующих совершению преступлений, а также в обязательном порядке, вносит в соответствующие государственные и коммерческие организации в порядке ч.2 чт. 158 УПК РФ о принятии мер по устранению обстоятельств или других нарушений закона;

15) осматривает, признает и приобщает к материалам уголовного дела в качестве вещественных доказательств имеющиеся выписки по движению денежных средств, ответы на направленные запросы, детализации телефонных переговоров, а также иные предметы и документы;

16) проводят иные следственные и процессуальные действия, необходимость в проведении которых может возникнуть в ходе расследования;

17) по окончании предварительного расследования и при выполнении всех следственных действий, возможных в отсутствии подозреваемого лица, принимает законное и обоснованное решение, при возникающей необходимости возбуждает перед руководителем следственного органа ходатайство о продления срока расследования;

18) в случае поступления ответа на запрос по приостановленному уголовному делу, незамедлительно знакомит с ним сотрудника уголовного розыска, и истребует от него рапорт о проверке данной информации по ИБД-Ф, которые помещает в материалы уголовного дела. При наличии признаком серийности, либо совпадений (абонентских номеров, IMEI-телефонов, номеров банковских карт преступников и т.д.) с другими территориальными ОВД РБ, истребует информацию, которая касается расследуемого уголовного дела, о чем уведомляет рапорта руководителя о возможном соединении уголовного дела в одно производство.

Таким образом, при проверке сообщения по факту совершения мошенничества с использованием информационно-телекоммуникационной сети Интернет требуется проведение всестороннего анализа имеющихся сведений, отработка следственных версий и проведение отдельных следственных действий.

§ 2. Взаимодействие следственных органов с органами дознания

Формы взаимодействия следователя как субъекта уголовно-процессуальной деятельности в расследовании мошенничеств с

использованием Интернет, существенно не отличается от общеуголовных преступлений, главным нормативно-правовым актом регламентирующим данную деятельность является, приказ МВД России от 21.07.2017 года №495 ДСП «Инструкция по организации взаимодействия подразделений и служб органов внутренних дел в расследовании и раскрытии преступлений». В соответствии с УПК РФ при расследовании и раскрытии преступлений следователь использует процессуальные и непроцессуальные формы взаимодействия.

Выбор конкретной формы взаимодействия, прежде всего, зависит:

1) от сложившейся следственной ситуации;
2) по информации, добытой по дежурным суткам;
3) характеристикой личности подозреваемого, обвиняемого;
4) сроком расследования;

Следователь и оперативные сотрудники осуществляют свою деятельность независимо друг от друга. Однако при решении совместных задач, вырабатывают согласованный план проведения оперативно-розыскных мероприятий и следственных действий, который утверждается начальником соответствующего подразделения.

Взаимодействия следователя и оперативных сотрудников, проявляется на двух относительно самостоятельных этапах:

1) на этапе проведение оперативно-розыскных мероприятий и следственных действий по поиску подозреваемого лица;

2) на этапе реализации оперативных сведений, полученных в ходе документирования;

В Республике Башкортостан организация взаимодействия органами предварительного следствия с оперативными службами ФСИН России осуществляется на основании совместного распоряжения ФСИН России по Республике Башкортостан и МВД по Республике Башкортостан №707/94р от 03.06.2015 года «О создании межведомственной рабочей группы по раскрытию и расследованию фактов мошенничества». Организация МВД по Республике

Башкортостан и ФСИН России, а также оперативного сопровождения и расследования уголовных дел находится на постоянном контроле у руководства ГСУ МВД по Республике Башкортостан.

Выполнение поручений следователя о проведении оперативно-розыскных мероприятий (п. 4 ч.2 чт. 38 УПК РФ и ч.3 ст.7, п.2 ст.14 Закон об ОРД) основывается на письменном задании с формулировкой ясных задач, выполнение которых требует применения оперативно-розыскных средств и методов).

На основании приказа от 22.07.2020 года №478 МВД по Республике Башкортостан был утвержден Алгоритм взаимодействия территориальных ОВД Республики Башкортостан при раскрытии и расследовании уголовных дел по мошенничествам и хищениям, совершенным с использованием информационно-телекоммуникационных технологий. оперативные сотрудники Министерства внутренних дел по Республике Башкортостан, исполняют поручения следователя о производстве отдельных следственных действий и оперативно-розыскных мероприятий, в рамках которого:

1. Принимает меры к принадлежности абонентских номеров, в том числе SIP-телефонии, используемых злоумышленником при совершении преступления, в том числе предварительно получает информацию о принадлежности абонентского номера к номерной емкости оператора телефонной связи, путем проверки по сервисным сайтам (http://kodtelefona.ru, smsc.ru, МГТС, сервисы Россвязи и другие).

2. Принимает меры к установлению реквизитов и наименование банка, который является эмитентом банковской карты преступника, куда потерпевший перевел денежные средства (по первым 6 цифрам на интернет ресурсах, например на сайте www.binlist.net, www.bincodes.com или bindb.com/bin-database.html.

3. Принимает меры к установлению на сайте «2ip.ru», информацию об ip-адресе либо домене (название сайта), с использованием которого осуществлялись преступные действия, организацию, зарегистрировавшую

доменное имя и оказывающую услуги хостинга сайту;

4. Готовить обобщенную справку по результатам проведенных оперативно-розыскных мероприятий, с отражением полученной информации, в том числе и о мероприятиях, связанных с проверкой на причастность к совершению преступления владельцев абонентских номеров и банковских карт;

5.Оказывает содействие следователю при направлении запросов на получении информации в различные организации, не требующие получения решений судов («Авито», «Вконтакте», «Одноклассники», «Майл.ру»).

6. Проверяет полученные, в ходе оперативно-розыскных мероприятий сведения об абонентских номерах, счетах, банковских картах, сайтах по ИБД-Ф с целью установления совпадений, при наличии совпадении связывается с территориальными отделами полиции УОМВД России, которыми внесена информация, для получения дополнительной данных, о чем докладывает рапортом на имя начальника ОВД в течение 3 суток с возможностью соединения уголовных дел в одно производство, полученные сведения также передает следователю для планирования отдельных следственных действий и оперативно-розыскных мероприятий;

7. Осуществляет поиск предметов, документов и иных носителей информации, которые могут быть признаны в вещественными доказательствами или иметь значение по уголовному делу;

8. Оказывает содействие следователю при производстве следственных действий (обыске, выемке, наложении ареста на имущество, доставлении и обработке лиц, причастных к совершению преступления, очевидцев его совершения и другие), осуществляет оперативное сопровождение до окончания расследования уголовного дела, оказывает необходимую помощь, в том числе подготовка запросов и истребование на них ответов.

При поступления поручения с целью установления принадлежности абонентского номера, направляет запрос посредством СЭД в канцелярию БСТМ МВД по РБ с указанием номера КУСП, УД регистрация абонентских номеров устанавливается, принадлежащей номерной емкости ПАО

«Вымпелком» по всей территории Российской Федерации, ПАО «МТС», ПАО «Мегафон» Приволжский федеральный округ.

В случаях, когда потерпевшие лично передавали денежные средства неустановленному лицу:

1) устанавливает подробные приметы лица; организует составление фоторобота преступника;

2) проводит мероприятия по установлению свидетелей и очевидцев совершенного преступления;

3) устанавливает наличие видеонаблюдения на месте преступления и по маршруту следования преступника, при наличии организовывает его немедленное изъятие;

4) проводит мероприятие по установлению транспортного средства, которое использовалось предполагаемым преступником для передвижения.

При поступлении поручений следователей из других территориальных ОВД РБ и субъектов РФ, обеспечивает полное качественное их исполнение в установленные сроки, а также полученные результаты (абонентские номера, номера счетов и банковских карт, которые использовали преступники) проверяет совпадение по ИБД-Ф.

Для получения наиболее полной информации по расследуемому уголовному делу, необходимо получения знаний от специалистов и экспертов в какой-либо деятельности. Следователь как процессуальное лицо, имеющие под своим контролем решения большинства задач в соответствии со своим положением, не обладает достаточными знаниями в криминалистической технике, естественных и технических наук. Вследствие этого, следователь взаимодействует с экспертами и специалистами в различных областях. В Российской Федерации деятельность экспертов регулируются в соответствии с Федеральным Законом от 31 мая 2001 № 73-ФЗ «О государственной судебной экспертной деятельности в Российской Федерации». Основным результатом взаимодействия следователя с экспертными учреждениями является проведение различного рода экспертиз.

В статье 196 Уголовно-процессуального кодекса Российской Федерации определены случаи, когда проведение экспертиз обязательно. Обстоятельства, устанавливаемые в процессе расследования мошенничеств в данный обязательный перечень не входит. Экспертиза по данному виду преступлений назначается когда установление обстоятельств дела с помощью других средств доказывания невозможно, а имеющиеся доказательства являются неполными и в них есть противоречия. Однако по мнению В.В. Агафонова и А.Г. Филлипова: «если при рассмотрении дела, есть возможность использования помощи специалистов такая возможность должна быть реализована»[1].

Процесс взаимодействия следователя с экспертом осуществляется на этапе подготовки следователем постановления о назначении экспертизы, в котором указывается: экспертное учреждение, которое будет проводит исследование, предмет экспертизы, конкретные основания и объекты.

В соответствии с УПК РФ заключение эксперта, а также его показания являются доказательствами по уголовному делу. В данном случае можно сделать вывод, что взаимодействие следователя с экспертами, специалистами является необходимым условием в процессе успешного расследования преступлений.

Таким образом, наиболее тесное взаимодействие следователя на этапе доследственной проверки и в процессе расследования преступлений осуществляется с органом, осуществляющим оперативно-розыскную деятельность. В качестве заключения следует отметить, что мошенничества с использованием Интернет носят межрегиональный характер. Налаженное взаимодействие с правоохранительными органами иных субъектов Российской Федерации с целью обмена информацией поспособствует более успешному раскрытию и расследованию данного вида преступлений.

---

[1] Агафонов В. В. Филлипов А.Г. Криминалистика: конспект лекций. М., 2018. С. 56.

ГЛАВА 3. ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

§ 1.Тактика проведения осмотра места происшествия

При поступлении сообщения о мошенничестве с использованием информационно-телекоммуникационной сети Интернет, обычно известны такие сведения: место нахождения заявителя в момент мошенничества, место перевода либо зачисления денежных средств.

При расследовании мошенничеств с использованием информационно-телекоммуникационной сети Интернет объектом осмотром места происшествия является местонахождение самого потерпевшего на момент перевода или зачисления денежных средств, местонахождение преступника на момент совершения мошеннических действий. В том случае, когда потерпевший находился по месту жительства с его согласия осмотр проводиться в жилом помещении. Осмотр места происшествия по данным видам преступлений проводиться по общим правилам, исключение составляет те случаи, когда в процессе совершения преступления использовались компьютеры, различного вида устройства.

В протоколе осмотра места происшествия необходимо указать следующие данные:

1) местонахождение компьютера (стационарный, планшет, ноутбук, смартфон), устройства связи (модем или роутер wi-fi), порядок их связи между собой (беспроводная или локальная сеть);

2) многозадачность каждого устройства: название, комплектация, серия и номер (сетевые карты, разъемы), присутствует ли на момент осмотра соединение с телекоммуникационной сетью, в каком состоянии находится.

Кроме того, при осмотре места происшествия могут изыматься системные блоки, либо накопители на жестких магнитных дисках, электронные носители данных, устройства связи. При изъятии электронных носителей необходимо

помнить о том, что они в соответствии с УПК РФ изымаются в присутствии специалиста. С письменного согласия заявителя при осмотре места происшествия следователем может производиться осмотр его мобильного телефона. По итогам осмотра, который целесообразнее проводить при участии специалиста, фиксируется следующая информация:

1) IMEI мобильного устройства заявителя.

В протоколе отображается следующим образом; «При извлечении аккумуляторной батареи, в корпусе телефона обнаружена конструктивная составляющая фотокамеры прямоугольной формы. Ниже фотокамеры расположена наклейка черного цвета на которой имеется текст: «IPHONE» модель: 8 IMEI 1 12486424811668;

2) абонентский номер SIM-карты заявителя;

3) тексты переписки между жертвой и мошенником по средством СМС-сообщений, мессенджеров «WhatsApp», «Viber». В данном случае, делается скриншот переписки, фотографии распечатываются и прилагаются к осмотру;
об использовании Интернет сервисов по виртуальному обороту платежных средств (электронные кошельки);

Если для осмотра мобильного устройства жертвы мошенничества требуется длительное время, специальные познания и технические средства, то в ходе осмотра места происшествия можно изъять мобильный телефон (и его содержимое), чтобы впоследствии провести отдельное следственное действие – осмотр предметов и документов.

В ходе осмотра жилища заявителя могут также изыматься имеющие значение для дела документы и сведения, которые потерпевший самостоятельно получил:

1) детализация входящих и исходящих соединений абонентского номера, с помощью которого заявитель контактировал с виновным;

2) выписки движения денежных средств по платежной карте, с которой были списаны деньги;

3) договор по открытию счета в банке (документы по оформлению

банковской карты, договор банковского обслуживания).

При проведении процессуальной проверки по сообщению о мошенничестве требуется провести осмотр места, где жертва преступления перевела денежные средства (если удалось установить – осмотр места зачисления денежных средств), которые были переданы на абонентский номер, банковскую карту, электронный кошелек. Как правило, в подобных случаях заявителем используется банкомат (платежный терминал самообслуживания). При осмотре места происшествия необходимо произвести осмотр помещения, где данные устройства установлены. В протоколе отражается наличие либо отсутствие камер наружного наблюдения, видеозаписи, а также факт перевода либо снятия наличных денежных средств заявителем. Помимо этого, фиксируется информация о лицах, подозреваемых в совершении мошенничества, их соучастниках, свидетелях, а также автотранспорте, который располагался в момент денежной операции у банкомата. Если камеры наружного видеонаблюдения имеются, тогда следователь обязан и изъять. Идентификационные номера на корпусе банкомата (платежного терминала) в последующем используются лицом, проводящем расследование, при направлении запросов администратору платежной системы (оператору сотовой связи) с целью подтверждения факта списания или зачисления денежных средств. В ходе осмотра места происшествия следователь (дознаватель) является руководителем следственно-оперативной группы, решает вопрос о привлечении дополнительных специалистов, определяет объем работы каждого участника, отвечает за сохранность следов, разъясняет права всем участникам следственного действия, несет персональную ответственность за результативность работы и достоверность отраженной в протоколе информации. Итогом обобщения и анализа такого массива работы является решение вопроса о возбуждении уголовного дела, принятие мер к установлению и задержанию подозреваемого в совершении дистанционного мошенничества лица.

Таким образом, осмотр места происшествия по заявлению (сообщению) о

мошенничествах, совершенных с использованием информационно-телекоммуникационной сети Интернет в большей мере нацелен на получение криминалистически значимой информации о механизме преступления, способе совершения, алгоритме действий злоумышленников, проверку имеющихся сведений с разработанными версиями. С учетом вышеизложенного, существует объективная необходимость в проведении такого следственного действия как осмотр места происшествия при расследовании данных видов преступлений. Оперативное и качественное его проведение может оказать определенный положительный результат при установлении преступника.

§ 2. Тактические приемы проведения обыска

Общие положения проведения обыска и выемки содержаться в ст. ст. 182 и 183 Уголовно-процессуального кодекса Российской Федерации. Так, согласно ст. 182 УПК РФ, основанием производства обыска является наличие достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия, оборудование или иные средства совершения преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела. И в соответствии со ст. 183 УПК РФ определённые предметы и документы, имеющие значение для уголовного дела, при необходимости могут быть изъяты. Производство обыска по делам о мошенничестве с использованием сети Интернет имеет свои особенности. Результаты анализа уголовных дел свидетельствуют о том, что в 14 % случаев при расследовании мошенничества с использованием сети Интернет проводился обыск. Производство обыска (выемки) при расследовании этой категории преступлений, связано с получением доказательств как способа совершения преступления, совершенного с использованием компьютерной техники и телекоммуникационных сетей.

Результаты проведенного обыска (выемки) по делам о мошенничестве в сети Интернет во многом зависят от подготовки к производству следственного

действия. Анализ уголовных дел выявил некоторые особенности производства обыска (выемки). Так, на подготовительном этапе обыска (выемки) следователю необходимо[1]:

1. Провести анализ имеющейся информации, выяснить в каких местах могут храниться доказательства;

2. Получить информацию о месте проведения обыска. Определиться со временем и участниками следственного действия. Анализ следственной и судебной практики показывает, что чаще всего место проведения обыска при расследовании мошенничеств с использованием информационно-телекоммуникационной сети Интернет является жилое помещение подозреваемого лица;

3. Изучить личность подозреваемого. Так, лицам, причастным к совершению мошенничеств с использованием информационно-телекоммуникационной сети Интернет, присуще попытка уничтожение доказательств, а также оказания сопротивления в процессе проведения обыска.

4. Подготовить материально-техническое обеспечение.

На рабочем этапе следователю необходимо:

1. Осмотреть все помещение. Применительно к данному виду преступлений технические средства являются орудиями и средствами преступлений, и возникает необходимость их первоначального обнаружения.

2. В случаях обнаружения на месте проведения обыска компьютеров, планшетов, смартфонов, данные средства осматриваются и изымаются (см.рис.2.3.1).

---

[1] Шевченко Е. С. Тактика отдельных следственных действий при расследовании кибер-преступлении // Закон и право. 2015. № 8. С. 128-138.

Рис.2.3.1.

Изъятые в ходе обыска компьютеры

3. Для поиска доказательственной информации совместно со специалистом для поиска в них нужной информации можно применить мобильный комплекс по сбору и анализу цифровых данных «UFED». С помощью этого мобильного комплекса можно извлекать данные на логическом уровне из большого количества устройств, извлекать журналы звонков, телефонную книгу, данные телефона (IMEI/номер телефона), SMS и MMS сообщения, фото и видеоизображения, звукозаписи, чаты, пароли, разблокировать пароль обыскиваемого устройства одним нажатием, выполнять быстрый поиск и фильтрацию данных по дате, времени, типу связи, лицу, использовать контрольные списки, просматривать события в хронологическом порядке и по карте, а также извлечь данные приложений и частного пользовательского облака. Так, в ходе обыска у К.Н.У. при личном обыске был изъят мобильный телефон, в котором содержались переписки с другими соучастниками данного преступления, а также иная значимая информация.

На заключительном этапе проведения обыска составляется протокол следственного действия и описи к нему. В протоколе описываются изъятые предметы и документы. В обязательном порядке указываются, сданы они добровольно или принудительно.

Таким образом, проведения такого следственного действия как обыск

является одним из способов получения доказательственной информации, необходимой для успешного раскрытия и расследования данного вида преступлений. А именно это изъятие электронных носителей информации и информации, которая храниться на компьютерах и электронно-вычислительных машинах.

§ 3. Тактические приемы проведения допроса

В целях выяснения наиболее криминалистически значимой информации, проведение такого следственного действия как допрос является необходимым элементом в процессе расследования данного вида преступлений. Показания потерпевшего традиционно содержат важную доказательственную информацию о личности мошенника (его внешности, приметах), месте, времени, способе совершения преступления, а также об особенностях имущества, которым завладел преступник.

Порядок проведения следственных действий зависит от конкретной сложившейся следственной ситуации. В ходе изучения уголовных дел было установлено, что наиболее часто допрашиваемыми лицами по расследуемому делу являются потерпевшие.

В первую очередь у потерпевшего устанавливаются следующие обстоятельства по делу:

Вопросы, направленные на установление ущерба:

1.1. Когда и каким способом потерпевший передавал денежные средства мошеннику? Сколько денег передавалось в каждом конкретном случае?

1.2. Есть ли свидетели, которые могут подтвердить факт отправки денежных средств мошеннику?

1.3. Сохранились ли документы, подтверждающие перевод денег?

2. Вопросы, направленные на установление конкретного способа совершения мошенничества и сокрытия следов преступления:

2.1. Кому принадлежала инициатива знакомства (другими словами, кто

кого раньше нашёл)?

2.2. Какую цель обозначил мошенник, на достижение которой потерпевший передавал деньги?

2.3. Что происходило после очередной пересылки и, особенно, после последней (переставал работать сайт мошенника и т.п.)?

2.4. После знакомства с мошенником, отмечал ли потерпевший случаи заражения своего компьютера вредоносными программами? Если такие случаи были, то сохранилась ли об этом информация на компьютере жертвы (например, в журналах антивируса)?

2.5. Проводила ли жертва чистку компьютера от ненужной информации? Если проводила, то каким способом и когда, а также с чем это было связано?

2.6. Не посылала ли жертва мошеннику дополнительную информацию о себе (например, фотографии, какую-либо финансовую информацию и т.д.)?

2.7. Есть ли у потерпевшего знакомые, которые контактировали с преступником?

3. Вопросы, направленные на получение информации о личности подозреваемого/обвиняемого, а также о возможных соучастниках:

3.1. Имела ли место переписка с мошенником? Какими способами она велась? Сохранились ли копии писем/сообщений?

3.2. Что потерпевший знает о преступнике? Каковы источники этих знаний?

3.3. Сколько раз потерпевший контактировал с Интернет- мошенником?

3.4. Зафиксирована ли информация о мошеннике в каких-либо носителях информации, принадлежащих потерпевшему (например, присланные мошенником фотографии, сохранённые в одной из папок на компьютере потерпевшего)?

3.5. Какую информацию о себе предоставлял мошенник? Как он представлялся потерпевшему? Какие вопросы задавал потерпевшему?

3.6. Сообщал ли Интернет-мошенник о местах (в т.ч. Интернет-сайтах и форумах), в которых он бывал?

3.7. Есть ли у потерпевшего и преступника общие знакомые, общее учебное заведение, общее прошлое и т.д.?

3.8. Проверяла ли жертва информацию, сообщённую мошенником?

3.9. Почему потерпевший поверил мошеннику и передал ему денежные средства?

3.10. Случались ли персональные встречи с мошенником, в том числе посредством видео-чатов? Если общение происходило при помощи видео-чата, то остались ли какие-либо свидетельства этого (скриншоты (снимки экрана), аудио- и видеозаписи общения)?

3.11. Интересовался ли мошенник во время переписки наличием у потерпевшего специальных познаний в какой-либо области, особенно, в области компьютерных технологий? Обладает ли жертва на самом деле такими познаниями?

В зависимости от того, как качественно следователь проведет допрос потерпевшего, зависит дальнейшее расследование уголовного дела. Поскольку информация передаваемая потерпевшим по мошенничествам, совершенных с использованием информационно-телекоммуникационной сети Интернет позволяется не только установиться обстоятельства случившегося, но и определить местонахождение лиц, совершивших преступления. Например, в Тюменской области в ходе расследования уголовного дела по факту мошенничества с использованием интернет-магазина, сайт которого впоследствии был заблокирован и недоступен при допросе потерпевших следователям удалось получить информацию о наименовании интернет-магазина, адресе, контактных данных, указанных на данном сайте, что способствовало установлению подозреваемых[1].

Так, К.Г. Михайлович указывает, что «следователь должен стремиться к тому, чтобы потерпевший свободно и осознанно избрал позицию,

---

[1] Приговор Ленинского районного суда г. Тюмени № 1-20/2019 1-718/2018 от 16 мая 2019 г. по делу № 1-20/2019 // Судебные и нормативные акты РФ. URL: https://sudact.ru (дата обращения: 04.04.2022).

направленную на оказание содействия в установлении истины по уголовному делу»[1]. При допросе потерпевшего, который стремится скрыть свой статус либо воспрепятствовать установлению истины по уголовному делу представляется целесообразным руководствоваться следующими рекомендациями. Проведение краткой беседы перед началом допроса на посторонние темы. Представляется, что данный прием применим ко многим видам допроса, поскольку позволяет получить представление о личности допрашиваемого, например, о его образовании, нравственных ценностях, образе жизни и т.д. Это позволит определить примерный перечень причин, по которым потерпевший не заинтересован в успешном расследовании дела.

В частности, следует объяснить потерпевшему о том, что его поведение может препятствовать защите его собственных прав и интересов. Если потерпевших несколько, представляется необходимым разъяснить, что своими показаниями потерпевший поможет не только быстрее и качественнее расследовать преступление, но и вернуть похищенное мошенниками не только себе, но и другим потерпевшим. В таком случае у допрашиваемого может возникнуть чувство позитивной ответственности перед другими потерпевшими, что позволит снизить противодействие следователю. Умеренно сочувствующее отношение со стороны следователя настроит на такое поведение и стиль общения следователя с потерпевшим, при котором у последнего создаётся устойчивое впечатление о том, что к расследованию его уголовного дела подходят серьёзно.

Несмотря на то, что следователь перед началом допроса указывает на возможность наступления ответственности, тем не менее, если охватывается ситуация, при которой взаимного доверия между следователем и допрашиваемым не возникло, то можно прибегнуть к акцентированию внимания последнего на том, что он, в какой-то мере, может из потерпевшего превратиться в обвиняемого, поскольку отказ от дачи показаний и дача

---

[1] Михайлович К. Г. Тактические и психологические основы допроса потерпевшего. Ижевск. 2016. С. 11.

заведомо ложных показаний влечёт наступление уголовной ответственности. Представляется, однако, что подобная информация, особенно высказанная в форме угрозы, может свести на нет все усилия следователя по созданию доверительных отношений с допрашиваемым.

Таким образом, к напоминанию об ухудшении положения потерпевшего следует прибегать только в крайних случаях. Если следователю становится очевидным, что потерпевший пытается скрыть необходимую для расследования информацию то, представляется возможным рекомендовать следующие тактические приёмы, которые позволят поставить допрашиваемого в такое положение, когда ему не останется ничего другого, как сказать правду:

1) изложение известных следователю событий в разной последовательности;

2) незаметное смещение акцентов при допросе (возможно лицо стало жертвой мошенничества из-за специфических увлечений, которые он предпочёл бы скрыть от посторонних, например, увлечение азартными играми на фоне работы с денежными средствами);

3) маскировка главного вопроса среди второстепенных;

4) просьба к потерпевшему от мошенничества максимально детализировать свои показания (например, как именно он узнал о сайте, который оказался мошенническим, почему он его искал, через какие запросы это происходило и т.д.);

5) предъявление имеющихся у следователя доказательств по расследуемому уголовному делу.

Проблема, с которой сталкивается, следователь при проведении допроса потерпевшего заключается в том, что жертва мошенничества зачастую не обладает достаточной информации, которая имеет значение для уголовного дела. Сбор и анализ показаний служит основой для создания качественной доказательственной информации по расследуемому уголовному делу. По тому, как следователь правильно, ясно и лаконично проведет допрос, зависит дальнейший исход дела. Поэтому, при проведении данного следственного

действия следователю необходимо прежде всего установить психологический контакт с допрашиваемым лицом.

Как перед проведением любого следственного действия следователю для проведения допроса необходимо провести ряд подготовительных этапов, тщательно знакомиться с материалами уголовного дела, с личностной характеристикой допрашиваемого лица в целях предотвращения возможного противодействия со стороны допрашиваемого лица, с учетом наличия у него значительного объема специальных знаний в сфере предмета допроса. В данном случае следует руководствоваться рекомендациями, рассмотренными ранее при допросе отдельных категорий лиц.

Допрос участников уголовного расследования является важным следственным действием, по результатам которого можно получить информацию обо всех элементах криминалистической характеристики преступления.

ЗАКЛЮЧЕНИЕ

Проведённое исследование особенностей расследования мошенничеств, совершенных с использованием информационно-телекоммуникационной сети Интернет позволило сформулировать следующие основные выводы:

1) в ходе написания данной работы были проанализированы: уголовно-правовая характеристика и элементы криминалистической характеристики мошенничеств, с использованием информационно-телекоммуникационной сети Интернет. Изучение всех элементов позволяет следователю выдвинуть следственные версии и определить тактику проведения следственных действий;

2) определены основные способы совершения преступления. Выделены наиболее распространенные способы совершения: преступления с использованием услуги «Мобильный банк» посредством мобильной связи; путем внедрения вирусов; путем обмана через звонок потерпевшему лицу; фиктивная продажа или покупка товаров, а также предоставление услуг. Необходимо отметить, что перечень способов совершения преступления не исчерпывающий, так как преступники придумывают все новые и новые способы;

3) проведение доследственной проверки по рассматриваемому виду преступлению позволяет следователю вынести мотивированное решение. Принцип проведения доследственнной проверки основывается на уголовно-процессуальных и криминалистических особенностях, а также на основе федеральных и ведомственных нормативных актах;

4) установлено, что в процессе расследования мошенничеств, совершенных с использованием сети Интернет важным элементом является установление в совокупности материальных и идеальных следов;

5) важную роль в процессе расследования и раскрытия данного вида преступлений является взаимодействия с органами дознания, а именно с оперативными сотрудниками, специалистами;

6) изучены личности потерпевшего и подозреваемого. Установлено, что

чаще всего преступниками являются лица мужского пола в возрасте от 18-30 лет (около 72 %), имеющих высшее или среднее образование.

В ходе написания работы изучены типовые характеристики тактики проведения допроса, осмотра места происшествия, а также обыска. Было сделано ряд выводов: определено, что чаще всего объектом осмотра места происшествия является место перевода денежных средств потерпевшего злоумышленнику; тактика проведения допроса строится на первоначальных исходных данных; анализ следственной практики показал, что обыск проводиться в 14 % расследуемых преступлениях.

В выпускной квалификационной работе проанализированы элементы криминалистической характеристики мошенничеств, совершенных с использованием сети Интернет, а также проведен анализ методики успешного проведения отдельных следственных действий и оперативно-розыскных мероприятий в процессе расследования и раскрытия преступлений.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – 16 июня.

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства РФ. – 2001. – № 52 (ч. I) – ст. 4921.

3. Досье на проект Федерального закона № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации (в части дифференциации мошенничества на отдельные составы)» // Гарант: информ.-правовой портал. URL: www.garant.ru (дата обращения: 04.04.2022).

II. Учебная, научная литература и иные материалы

1. Агафонов В. В. Филлипов А. Г. Криминалистика: конспект лекций. М., 2018. 134 с.

2. Бессонов А. А. О сущности криминалистической характеристики // Вестник Поволжской академии государственной службы. 2014. № 6 (45). С. 48.

3. Большакова В. Н. Разграничение криминалистических понятий: модель преступления, поисковый портрет преступника, криминалистическая характеристика преступлений // Пробелы в российском законодательстве. 2014. № 3. С. 52-56.

4. Возгрин И. А. Криминалистическая методика расследования преступлений. Минск, 1983. 394 с.

5. Давыдов В. А. Цифровые следы в расследовании интернет-мошенничества // Вестник Краснодарского университета. 2015. № 2. С.13-16.

6. Зуева С. В. Основы теории электронных доказательств: монография. М: Юрлитинформ, 2019. 59 с.

7. Карагодин В. Н. Расследование преступлений совершенных организованными формированиями. М., 2017. 165 с.

8. Козлов В. Е. Теория и практика борьбы с преступностью. Москва, 2017. 123 с.

9. Майоров В. И. К вопросу о порядке рассмотрения сообщения о преступлении // Проблемы и вопросы уголовного права, уголовного процесса и криминалистики. 2017. № 2. С. 31-33.

10. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. ...д-ра юрид. наук. Воронеж, 2016. С.75-79.

11. Мещеряков В. А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. Научный журнал. 2013. № 5. С. 269-272.

12. Михайлович К. Г. Тактические и психологические основы допроса потерпевшего. Ижевск, 2016. 180 с.

13. Никулин Д. В. Жертвы мошенничества. // «Научно-практический электронный журнал Аллея науки». 2018. № 1. Ст. 10.

14. Никульченкова Е. В. Мошенничество проблемные вопросы // Вестник Омского университета. Серия «Право». 2016. № 2. С. 160-165.

15. Олиндер Н. В. Время и место совершения преступления как элемент криминалистической характеристики преступлений, совершенных с использованием электронных платежных средств и систем // Науковедческие проблемы криминалистики. 2018. № 4. С. 17-19.

16. Потапова А. В. Мошенничество в сети интернет: криминологическая характеристика и проблемы квалификации. Научно-образовательный журнал для студентов и преподавателей. // Право. 2020. № 5. (дата обращения: 04.04.2022). С. 54-46.

17. Рарога. А. И. Уголовное право России: две части. М., 2016. 145 с.

18. Романова Л. И. Личность интернет-преступника // Азиатско-Тихоокеанский регион: экономика, политика и право. 2018. № 3. С.159-169.

19. Русаков И. М. Криминалистическая характеристика личности преступника, совершившего мошенничество в сфере предоставления интернет-услуг // Вестник Краснодарского университета МВД России. 2015. № 4.

С. 45-49.

20. Семикаленова А. И., Рядовский И. А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019, №6 (103). С. 178-184.

21. Состояние преступности в России. МВД РФ ФКУ «Главный информационно-аналитический центр». Москва, 2022. 185 с.

22. Степанов В. В., Бабаков М. А. Поисково-познавательная деятельность при расследовании преступлении, совершенных с использованием высоких технологий: монография. М.: Юрлитинформ, 2014. 152 с.

23. Тарубаров В. В. Общественные места как участки местности с повышенной социальной опасностью // Вестник Московского университета МВД России. 2018. № 1. С. 115.

24. Шевченко Е. С. Тактика отдельных следственных действий при расследовании киберпреступлении // Закон и право. 2018. № 8. С. 128-138.

III. Эмпирические материалы

1. Приговор Туймазинского межрайонного суда Республики Башкортостан от 18.04.2019 № 1-30/2019 // URL: https://sudact.ru (дата обращения: 04.04.2022).

2. Приговор Ленинского районного суда г. Тюмени № 1-20/2019 1-718/2018 от 16 мая 2019 г. по делу № 1-20/2019 // Судебные и нормативные акты РФ. // URL: https://sudact.ru (дата обращения: 04.04.2022).

3. Решение Калининского районного Суда г. Челябинска (Челябинская область) от 18.04.2018 г. № 2а-1975/2018. // URL: https://sudact.ru (дата обрашения: 04.04.2022).

4. Приговор Орджоникидзевского районного суда г. Новокузнецка Кемеровской области № 1-26/2019 1-362/2018 от 15 февраля 2019 г. по делу № 1-26/2019 // Судебные и нормативные акты РФ. // URL: https://sudact.ru (дата обращения:04.04.2022).

5. Уголовное дело № 119…111 // Арх. СО ОМВД России по Туймазинскому району. С. 3-19.

6. Приговор Советского районного суда г. Уфы Республики Башкортостан № 1-26/2019 1-362/2018 от 07 мая 2019 г. по делу № 1-26/2019 // Судебные и нормативные акты РФ. // URL: https://sudact.ru (дата обращения: 04.04.2022).

7. Уголовное дело № 119…118 // Арх. СО ОМВД России по Туймазинскому району. С. 5-18.

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну.

Д.Л.Аглетдинова